Парсер Syslog Regex

Общие сведения

В AxelNAC подержано создание синтаксического анализатора системного журнала (Syslog) с помощью регулярных выражений. Это, в свою очередь, позволит создавать сложные фильтры и правила для работы с данными, получаемыми через журнал.

Для создания парсера перейдите в раздел **Конфигурация → Интеграция → Парсеры Syslog → Новый парсер Syslog** и выберите значение **Regex** в выпадающем списке.

На открывшейся странице вы можете выполнить следующие настройки:

- **Детектор** — укажите идентификатор детектора, который будет использоваться;
- **Статус** — работу парсера можно включать и выключать;
- **Канал уведомлений** — укажите ранее созданный канал оповещений (FIFO);
- **Правила** — список правил, определяющих, как сопоставлять записи в журнале и какие действия предпринимать при сопоставлении. Правила парсера:
  - **Имя** — имя правила;
  - **Regex** — регулярное выражение для сопоставления с записью журнала. Может иметь именованные захваты которые можно использовать для замены параметров, начинающихся с '$'.
  - **Действия** — список действий, которые необходимо выполнить при совпадении регулярного сообщения;
  - **Остановить, если совпадает** — остановить обработку других правил, если это правило совпадает;
  - **IP ⇄ MAC** — автоматическая трансляция IP-адресов в MAC-адреса и наоборот.

Определение действий

Действие состоит из двух частей:

Метод — имя действия, которое необходимо выполнить;
Список параметров — список параметров, которые необходимо передать методу. Каждый параметр разделяется запятой. Параметры, которые должны быть заменены именованным захватом.

Пример действия:

Regex:
macs*: s* (? P< mac> [a-zA-Z0-9] {2} (: [a-zA-Z0-9] {2}) {5}), notess*: s* (P?< notes>.*)
Действие:
modify_node: mac, $mac, notes, $notes

ID статьи: 598
Последнее обновление: 17 июл., 2024
Обновлено от: Егоров В.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство администратора -> Интеграция с системами обнаружения вторжений (IDS) -> Парсер Syslog Regex
https://docs.axel.pro/entry/598/